AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

United States of America
v.
Uju OKIGBO (a/k/a "Uju Ernest")

Case No. H17-1735

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of November 2014 - present in the county of Fort Bend and Harris in the Southern District of Texas, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. Section 1956(h)	Conspiracy to Commit Mondey Laundering

This criminal complaint is based on these facts:

See attached affidavit in supprort of criminal complaint.

☑ Continued on the attached sheet.

Complainant's signature

SA John Chiue, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: November 14, 2017

Judge's signature

City and state: Houston, Texas

Hon. Frances H. Stacy, Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, John Chiue, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint establishing probable cause for the arrest of Uju OKIGBO (a/k/a "Uju Ernest") for committing the following offense in the Southern District of Texas and elsewhere from in or about November 2014 until present: conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h).

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and am a federal law enforcement officer within the meaning of Rule 41(h), Federal Rules of Criminal Procedure. I have been employed with the FBI since 1991. I am currently assigned to the Organized Crime Squad which has as one of its primary functions the identification and investigation of complex financial fraud schemes and money laundering. As an FBI agent, I have participated in numerous financial investigations involving the laundering of proceeds from various types of fraud, the sale of narcotics, and human smuggling/trafficking activities.

3. This affidavit is intended to show merely that there is sufficient probable cause for the complaint and does not set forth all of my knowledge about this matter. The information contained in this affidavit is known to me personally or is based on my review of documents, reports, or information told to me by witnesses and other law enforcement officers.

OVERVIEW OF FRAUDULENT SCHEME AND ASSOCIATED LAUNDERING

4. As detailed in this affidavit, there is probable cause to believe that OKIGBO knowingly joined a conspiracy to commit money laundering. OKIGBO is a citizen of the United States currently residing in Richmond, Texas. For over two years, OKIGBO laundered the

proceeds of an international advance-fee scam through her bank accounts. The scam committed by OKIGBO's co-conspirators involved falsely promising victims investment funding, supposedly offered by "Bank A," a U.S. bank headquartered in North Carolina, and supposedly sponsored by the U.S. government, in exchange for paying various fees (hereinafter, the "Bank A scam"). I have found victims in, among other places, Mongolia, Canada, Denmark, South Korea, Colorado, and Texas.

5. At co-conspirators' instructions, the victims wired the fees to, among other places, bank accounts under OKIGBO's control in the Southern District of Texas. To deceive the victims into believing the investment funds were legitimate, co-conspirators impersonated real U.S. bank officials and U.S. government employees in emails, phone calls, documents, and in-person meetings. The co-conspirators also created fraudulent U.S. State Department letterheads and receipts, and other U.S. government documents to dupe victims into believing the investment agreements were legitimate. As detailed below, there is probable cause to believe that OKIGBO, by opening bank accounts to receive proceeds of the Bank A scam and then withdrawing and transferring those funds or using them to purchase cars that were then shipped to Nigeria, joined a conspiracy to launder the proceeds of criminal activity.

6. I have reviewed evidence including witness interviews, audio recordings, and financial records, as described in more detail below, which all indicate that OKIGBO continued to open bank accounts to receive proceeds of the fraud even as those accounts were flagged and closed by banks for suspicious account activity.

MONGOLIAN VICTIMS

7. In course of this investigation, I interviewed two individuals in Mongolia who were victims of the Bank A scam, Mongolian victim #1 and Mongolian victim #2. They

informed me that sometime in late 2014, an individual impersonating Executive #1,[1] a Senior Executive Vice President of Bank A, contacted Mongolian victim #1 via email. Executive #1 introduced, via email, an "Assistant" and Impersonator #1 as her associates who could assist Mongolian victim #1 in securing financing for a business venture.

8. According to the Mongolian victims I interviewed, in or about November 2014, Impersonator #1 traveled to Mongolia. On or about November 12, 2014, Impersonator #1, claiming to represent Bank A, signed a supposed investment agreement with Mongolian victim #1. The supposed purpose of the investment agreement was for Bank A to transfer $22.5 million into Mongolian victim #1's account for investment projects in Mongolia. A representative of Bank A has verified to me that Impersonator #1 has never been a Bank A employee, that Bank A never entered into such an agreement in Mongolia, and that the real Executive #1 has never been in contact with these investors in Mongolia.

9. According to the Mongolian victims I interviewed, on or about November 13, 2014, Impersonator #1 collected $5,000 in cash from Mongolian victim #1 as a notary fee and went to the U.S. Embassy in Ulaanbaatar, Mongolia. Impersonator #1 entered the U.S. Embassy and returned with an agreement supposedly notarized by the Embassy and a receipt bearing the seal of the U.S. Department of State apparently indicating a notary fee of $5,000 paid to the U.S. Consulate General. (The U.S. Embassy visitors' log, which I have reviewed, indicates that Impersonator #1 visited the American Citizen Service Section on November 13, 2014.) Consular officials have verified that the receipt was fake.

---

[1] Any time I refer to "Executive #1" I am referring to the individual impersonating Executive #1, not the real Executive #1.

10. The fraudulent agreement required the investors to pay $385,000 in administrative fees prior to the transfer of the $22.5 million investment fund. According to the Mongolian victims I interviewed, the victims were not immediately able to pay this fee. Also, the victims started to question the validity of the funding by Bank A. Executive #1 told the victims that she would be sending another bank representative, referred here as Impersonator #2, to Mongolia to reassure the victims.

11. According to the Mongolian victims, in on or about January 2015, Impersonator #2 traveled to Mongolia. I have reviewed a photo of Impersonator #2 taken by one of the Mongolian investors while Impersonator #2 was in Mongolia. The individual in the photo matches the person appearing in Impersonator #2's authentic U.S. passport, a copy of which was forwarded to the Mongolian investors in advance of Impersonator #2's visit

12. According to the Mongolian victims, they gave Impersonator #2 $10,000 as payment for a rescheduling fee due to the delay. On or about January 22, 2015, Impersonator #2 went to the U.S. Embassy in Ulaanbaatar and returned with a receipt supposedly showing payment of $10,000 to "U.S. Consul General" for "Reschedulment [sic] and PPT Security fees." (The U.S. Embassy visitor's log indicates that Impersonator #2 visited the American Citizen Service Section on or about January 22, 2015.) Consular officials have verified that the receipt, like the one provided by Impersonator #1, was fake.

13. A few weeks after Impersonator #2's visit, the Mongolian victims were told to start making additional payments towards the bogus fees they had to pay. According to the investors and bank records I have reviewed, the investors made the following wire transfers to a bank account ending in 3778 in the name of U-4CS Services, opened at a Bank A branch in

Sugar Land in the Southern District of Texas ("Bank A Account #1"), on the false belief these were necessary fees to complete the investment agreement:

Date	Amount	
2/9/15	$25,000	
2/17/15	$150,000	
2/26/15	$175,000	
3/11/15	$100,000	
3/13/15	$50,000	
3/17/15	$60,000	
3/18/15	$40,000	
4/14/15	$20,000	
4/14/15	$160,000	
4/16/15	$20,000	
4/22/15	$85,000	
4/28/15	$95,000	
	$980,000	**TOTAL**

14. According to the Mongolian investors I interviewed, on or about February 22, 2015, Impersonator #1 again traveled to Mongolia and met with the Mongolian victims. As part of her visit, she provided the Mongolian victims with various fraudulent documents, including additional certificates supposedly produced by Bank A and documents supposedly showing that the U.S. Department of State, and particularly the U.S. Embassy in Ulaanbaatar, was guaranteeing the investment project. I have verified that these documents were false by speaking with staff at the U.S. Embassy and representatives of Bank A.

15. The Mongolian victims eventually realized that the investment agreement was a fraud and the Mongolian National Police took Impersonator #1 into custody in May 2015, soon after she arrived on her third trip to Mongolia in furtherance of the fraud. Mongolian victim #1 was also arrested, convicted and sentenced in Mongolian court for "swindle" due to his inability

to repay the loans he had taken to pay for fees associated with the fraud. According to conversations I had with the Mongolian authorities, during the post-arrest interview by the Mongolian authorities, Impersonator #1 insisted that she was employed by Bank A and that her boss was the Assistant.

16. To date, the Mongolian victims have paid over $2 million as part of the scheme and not received any money from Bank A, the Assistant, Executive #1, Impersonator #1, or Impersonator #2.

CANADIAN VICTIM

17. In the course of my investigation, I learned of a Canadian resident who was a victim of the Bank A scam (the "Canadian victim"). I requested that the Royal Canadian Mountain Police (RCMP) interview the Canadian victim, which they did on two occasions, the first time in October 2015 and the second time in May 2017. I received transcripts of those two interviews from the RCMP. The Canadian victim is the owner of Company #1 based in Alberta, Canada. In both interviews the Canadian victim stated that he had made payments to Bank A Account #1 from the bank account of Company #1. In the first interview the Canadian victim claimed the payments to Bank A Account #1 were for solvents purchased for his business, while in the second interview he admitted the payments were part of a fraudulent Bank A investment agreement he had signed and that Impersonator #1 had visited him under the pretense of singing the investment agreement. He stated that he had initially lied to the RCMP about having been a victim because he was embarrassed about having been defrauded.

18. According to bank records I have reviewed, from in or about December 2014 through in or about February 2015, the Canadian victim wired approximately $563,180 to Bank

A Account #1 from the bank account of Company #1. To date, the Canadian victim has not received any money from Bank A, Executive #1, or Impersonator #1.

AUSTRALIAN VICTIM

19. In the course of my investigation into the Bank A scam, I interviewed an Australian citizen who resides in Melbourne, Australia (the "Australian victim"). The Australian victim told me that he had been introduced via email to Executive #1 of Bank A, which was supposedly looking for a partner in an investment project worth $35 million. In or about February 2015, Impersonator #1, the same individual who traveled to Mongolia and Canada, came to Melbourne to sign the supposed investment agreement on behalf of Bank A. The Australian victim drove Impersonator #1 to the U.S. consulate supposedly so the U.S. government could ratify the agreement. The Australian victim paid $5,000 to Impersonator #1 supposedly as a fee for the U.S. government to ratify the agreement, and when Impersonator #1 exited the consulate she gave the Australian victim a supposed receipt for the $5,000 payment to the consulate.

20. After the agreement was signed, the Australian victim received emails from Executive #1 requesting certain payments so that the $35 million investment fund could be released. The Australian victim made two wire payments to Bank A Account #1 totaling approximately $130,000. With at least one of those payments, sent on or about February 13, 2015 in the amount of $36,695, the Australian victim attempted to recall the wire after he had initiated it, but was convinced by Executive #1 to cancel the recall. The Australian victim never received any money from Executive #1, Impersonator #1, or Bank A, nor did he receive back any of the approximately $135,000 he paid in the course of the scam.

DANISH VICTIM

21. In the course of my investigation into the Bank A scam, I also interviewed a victim living in Denmark (the "Danish victim"). The Danish victim informed me that he had been the victim of an earlier advance-fee scheme in 2014 in which he had lost approximately $720,000, all in the hope of being the beneficiary of a $20 million investment fund. The Danish victim maintained hope that he could recover the money he had spent. In connection with the previous scam, the Danish victim received an email telling him to contact Executive #1, who the Danish victim believed was a Senior Executive Vice President at Bank A and who could supposedly help him recover his money.

22. According to the Danish victim, on September 2015, the Danish victim met with Impersonator #2 in Copenhagen believing that Impersonator #2 was an employee of Bank A and would be signing an investment agreement with the victim on behalf of Bank A and Executive #1. The purported purpose of the investment agreement was for Bank A to transfer $20 million into the account of the Danish victim for investment projects in Demark. The investment agreement was supposedly signed by Executive #1 and contained a supposed notary seal from the U.S. Embassy in Copenhagen, Demark.

23. According to the Danish victim, on or about September 22, 2015, the Danish victim drove Impersonator #2 to the U.S. Embassy in Copenhagen, Denmark. The Danish victim then paid Impersonator #2 $10,000 as a supposed notary and administrative fee. Impersonator #2 provided a receipt that was supposedly from the U.S. Consulate General, Copenhagen, Denmark. The receipt appeared similar to the ones used to perpetrate the fraud in Mongolia, and thus was also false. I reviewed surveillance footage provided by the U.S. Embassy in Copenhagen which showed someone matching the appearance of Impersonator #2 entering the

Embassy at approximately 11:30am, sitting in the waiting area of the consular services section for approximately 20 minutes, and then exiting the Embassy.

24. On or about September 25, 2015, the Danish victim transferred $25,000 (in the form of two $12,500 wires) to Bank A Account #1, and had the intention of transferring the remaining amount of $225,000 believing the investment agreement was legitimate. However, the Danish victim went to the U.S. Embassy in Copenhagen, Denmark to verify the authenticity of the embassy stamp on the supposed agreement. There, the Danish victim learned the stamp was fraudulent and the attorney listed on the investment agreement did not exist. The Danish victim never received any money from Bank A, Executive #1, or Impersonator #2, nor did he receive back any of the money he paid in the course of the scam.

KOREAN-AMERICAN VICTIM

25. In the course of my investigation into the Bank A scam, I interviewed a Korean-American dual citizen who resides in Seoul, Korea and who was also a victim of the scam (the "Korean-American victim"). He informed me that sometime in 2015 he was introduced over the Internet to someone he believed was Executive #1 of Bank A, who offered him investment funding on behalf of Bank A. He was told that two individuals would travel to Korea to sign the investment agreement with him. These individuals, Impersonator #3 and Impersonator #4 (acting in roles similar to Impersonator #1 and Impersonator #2), did travel to Korea in late 2015. They were not actually employees of Bank A, a fact which I verified with Bank A representatives.

26. According to the Korean-American victim, Impersonator #3 and Impersonator #4 signed the investment agreement on behalf of Bank A. The victim had been instructed by Executive #1 to pay the Impersonators $7,500 as a processing fee. The Impersonators also

requested that they be brought to the U.S. Embassy in Seoul so the agreement could supposedly be processed.

27. According to the Korean-American victim and bank records I have reviewed, after the investment agreement was signed, Executive #1 started requesting that the victim make payments to bank accounts in the United States, including two accounts in the name of U-4CS Services located in the Southern District of Texas. Because the victim did not have the funds to make the payments, he recruited business partners for what he believed was a legitimate investment venture.

28. According to information supplied by the Korean-American victim, as well as bank records I have reviewed, on or about January 7, 2016, the victim and his associates made a $50,000 wire payment to an account at Bank B ending in 3244, in the name of U-4CS Services ("Bank B Account #1"). On or about January 13, 2016, the victim and his associates made a $36,000 wire payment to a Bank A account in the name of U-4CS ending in 8992 ("Bank A Account #2").

29. In March and April 2016, the Korean-American victim and his associates made additional payments in the amount of $14,872 and $55,000 to Bank A Account #2. In total, from December 2015 through April 2016, the victim and his associates wired approximately $156,000 to Bank B Account #1 and Bank A Account #2. Neither the Korean victim nor his associates every received any money from Impersonator #3, Impersonator #4, Executive #1, or Bank A.

SUMMARY OF ROLE OF OKIGBO

30. As detailed in the paragraphs below, all of the Bank A scam victims discussed above wired funds into bank accounts opened and controlled by OKIGBO, who would quickly

withdraw the funds, often to purchase vehicles that she then shipped to Nigeria. In this way, OKIGBO laundered the proceeds of the Bank A scam on behalf of its perpetrators.

BANK A ACCOUNT #1 ACTIVITY

31. According to bank records I have reviewed, Bank A Account #1 was opened by OKIGBO[2] on December 1, 2014 at a Bank A branch in Sugar Land, Texas. The day after the account was opened, December 2, 2014, it received a $100,000 wire transfer from a Canadian bank account controlled by the Canadian victim (mentioned in paragraphs 17 and 18) and in the name of his company. The following day, December 3, 2014, a second $100,000 wire transfer from the same Canadian account was sent to Bank A Account #1.

32. Two days later, on or about December 5, 2015, OKIGBO wired $170,000 of the funds to a title company in Texas. According to records I obtained from the title company, those funds were used by OKIGBO to purchase a house for herself in Richmond, Texas. Virtually all $170,000 were proceeds of the Bank A scam, as only $300 in cash had been deposited in the account when it was opened days earlier. An additional wire in the amount of $40,000 was sent the following month to the title company from Bank A Account #1. Those funds were also proceeds of the Bank A scam: almost all the deposits during the first six weeks after Bank A Account #1 had been opened were from the Canadian victim's wire transfers.

33. According to bank records, additional proceeds of the Bank A scam were withdrawn in the form of personal checks and cashier's checks, often to purchase vehicles. For example, I have located the following checks drawn off Bank A Account #1 in the days following deposits from the Canadian victim:

---

[2] In or about April 17, 2016, according to DMV records I have reviewed, OKIGBO changed her name from Uju Ernest to Uju Okigbo. Thus, Bank A Account #1 was actually opened in the name of Uju Ernest.

a. a $5,000 check dated January 20, 2015 with the memo line "2007 Toyota Camry" following a $55,000 wire transfer on January 13, 2015;

b. a $15,000 check dated January 26, 2015 with the memo line "Payment for 2010 Honda Crosstour" and a $40,000 check dated January 29, 2015 with the memo line "Payment for Cars," both following a $120,000 wire transfer on January 22, 2015;

c. a $19,000 check dated February 11, 2015 with the memo line "Payment for Cars" following a $100,000 wire transfer on February 10, 2015; and

d. a $4,655 check, dated February 13, 2015, with the memo line "Payment for 2007 Honda Accord" following a $15,700 wire transfer on February 12, 2015.

34. A similar pattern emerged for the payments from the Mongolian victims, an example of which is set forth below:

a. A $17,000 check dated February 18, 2015, with the memo line "Payment for cars," a $60,000 check dated February 20, 2015, with the memo line "Payment for cars," and a $14,888.31 check dated February 23, 2015, with the memo line "Payment for 2010 Honda Crossover," all following a $149,990 wire transfer dated February 17, 2015 from the Mongolian victims.

35. Bank records show that there were also thousands of dollars of cash withdrawals and debits at Sam's Club, TJ Maxx, Macy's, and other retailers.

36. As noted earlier, the Australian victim attempted to recall one of the wires sent to Bank A Account #1, on or about February 13, 2015 in the amount of $36,695. According to bank records I received, OKIGBO denied the request to return the wire.

37. I have interviewed a customer service representative at Bank A who handled the wire recall. According to the representative, when the sender of a wire transfer recalls a wire, the

receiving bank—here, Bank A—contacts the recipient of the wire and inquires whether the recall will be accepted or denied. Here, the representative phoned OKIGBO, who came into the Bank A branch where the representative worked and signed the form denying the recall request. OKGIBO claimed that her "boss" was in communication with the sender of the wire and had worked it out with his "client" (i.e., the Australian victim who was in communication with Executive #1 but who never received anything).

BANK A ACCOUNT #2 ACTIVITY

38. On or about December 24, 2015, Bank A Account #1 was closed due to fraud. I spoke to the Bank A customer service representative who spoke with OKIGBO on the day Bank A Account #1 was closed. The representative said the account was closed due to external fraud or account compromise, and that same day OKIGBO opened Bank A Account #2.

39. Soon after OKGIBO opened the account, foreign wire transfers from victims of the Bank A scam started arriving in the account. For example, on or about January 14, 2016, the Korean-American victim and his associates wired $36,000 to Bank A Account #2. Those funds were withdrawn immediately. For example, on or about January 15, 2016, $28,000 was withdrawn: $8,000 in cash, and $20,000 in a cashier's check made out to "Quality Ingredients" with the memo line "Payment for Goods."

40. From January 2016 until April 2016, several hundred thousand dollars of wire transfers from victims arrived in the account, including from the Korean-American victim and his associates.

41. On or about April 25, 2016, the BSA/AML [Bank Secrecy Act/Anti-Money Laundering] section of Bank A decided to close Bank A Account #2 and terminate its banking relationship with OKIGBO. It sent a letter to OKIGBO notifying her of this and giving her 30

days to withdraw the balance from the account. I have reviewed the letter. It states: "Due to the confidential nature of the information that led to this decision, our branch or other bank personnel will not be able to discuss specific reasons for closing your account."

BANK A ACCOUNT NOTICES

42. I know from bank records that Bank A has a practice of sending account holders a letter detailing "Wire Transfer Operations" whenever an incoming or outgoing wire transfer is completed. Those letters are sent to the address on file for the account holder and include information such as the amount wired, receiving account number, the originating bank name, the originating account holder, and a memo accompanying the transfer. The address on file was the one for the house OKIGBO purchased in early 2015 with proceeds of the Bank A scam.

43. According to my review of those letters for Bank A Account #1 and Bank A Account #2, none of the incoming wires from victims of the Bank A scam mentioned anything about goods or payments for cars; only the outgoing checks and wires did. Rather the memos for the incoming wires included text such as "Payment for Administrative Charges and Court Documents," "The Waiver Fee Payment of Administrative Charge," "The Payment of Data Transfer Processing Fee," "Commitment Fee," and "Legal Fee," which are the memos provided by victims of the Bank A scam.

BANK A CALL WITH OKIGBO

44. On or about May 5, 2016, an investigator with Bank A called OKIGBO to ask questions about Bank A Account #1 and Bank A Account #2, and the incoming and outgoing wires. This call was recorded. I have listened to the recording. During the call, the Bank A investigator asked OKIGBO whether she knew the individuals wiring money into her account.

OKIGBO responded that she knew the "clients" and that the incoming payments were for goods and cars, which she would purchase and then ship to Nigeria.

45. From my conversations with the victims of the Bank A scam, I know that none of them know OKIGBO or have ever spoken with her. Therefore, OKIGBO's statements to the Bank A investigator about knowing the individuals wiring her money were false.

BANK B ACCOUNT #1 ACTIVITY

46. Prior to opening the Bank A Account #1, OKIGBO already had an account in the name of U-4CS, but at Bank B (i.e., Bank B Account #1). According to bank records I have reviewed, the account was opened on June 7, 2013.

47. The first time victim's money was transferred into the account was December 23, 2015, approximately one day before Bank A Account #1 was closed and Bank A Account #2 was opened.

48. The account received additional wires from victims in January and February 2016. The proceeds were withdrawn in a similar fashion to the other accounts: via cash withdrawals and cashier's checks with notations about car purchases.

49. The account was closed by Bank B on May 18, 2016.

BANK B ACCOUNT #2 ACTIVITY

50. After Bank A Account #1, Bank A Account #2, and Bank B Account #1—December 24, 2015, April 26, 2016, and May 18, 2016—were closed, on or about May 18, 2016, OKIGBO opened another Bank B account in the name of U-4CS, this one ending in 7028 ("Bank B Account #2). Almost immediately after the account was opened, victims' payments started flowing into it, the first one on May 26, 2016. Similar to the other accounts, as captured in the

bank records, the funds were immediately withdrawn after they appeared in Bank B Account #2, principally to purchase cars.

51. According to bank records, an incoming wire in the amount of $200,015 on September 15, 2016 from an American victim of the Bank A scam, whom I have spoken to, raised a red flag at Bank B, and resulted in a freeze being placed on the account.

52. On or about September 26, 2016, OKIGBO called Bank B to inquire about the account freeze. That call was recorded in the ordinary course of Bank B's business, and I have listened to it. She was told that the incoming wire had triggered the freeze.

53. Following the account freeze, Bank B Account #2 had minimal transaction activity until the account was closed on or about March 2, 2017.

BANK C ACCOUNT

54. According to bank records I have reviewed, on or about September 1, 2016, OKIGBO opened another business bank account in the name of U-4CS Services, this one ending in 7218 at a "Bank C" branch in Houston (the "Bank C Account").

55. According to bank records, the Bank C Account had no activity (aside from an opening deposit) until on or about November 17, 2016, when the Bank C Account received a wire from the United Arab Emirates (UAE) in the amount of $24,945. The wire was from a victim of the Bank A scam. According to a report from Bank C, Bank C's OFAC [Office of Foreign Assets Control] department flagged the wire payment because the UAE is deemed a high-risk country. Bank C reached out to OKIGBO to inquire as to the purpose of the payment.

56. According to records from Bank C, OKIGBO replied that the payment was for the export of a vehicle, and provided Bank C with the copy of a document supposedly showing that a company named "PT. Chaerul Research Int" was acting as an agent for U-4CS Services and

another company whose name began with "Atlas." When an employee at Bank C asked for a copy of the passport of the company's director, OKIGBO requested that the wire from the victim be returned.

57. No more wires were sent to Bank C Account after the above-mentioned wire was cancelled.

BANK D ACCOUNT

58. According to bank records I have reviewed, on or about November 17, 2016, OKIGBO opened another bank account in the name of U-4CS Services LLC, this one at "Bank D" ending in 2876 (the "Bank D Account")—even though four prior accounts in the same name had been closed by two banks in the previous year following the account activity of receiving (mostly) international wires and then immediately withdrawing the funds to (mostly) purchase cars.

59. The first wire transfer to arrive in the account was approximately one week later, on or about November 25, 2016, in the amount of $20,000 from an account in Florida. The message accompanying the wire transfer was, "Deposit as far [sic] [Bank A]," indicating that the transfer was likely from another victim of the Bank A scam.

60. The next wire transfers into the Bank D Account were on December 9, 2016 and December 12, 2016, and were from the same victim who had attempted to send the $24,945 wire into the Bank C Account, which Bank C ended up returning. The December wires from the victim again mentioned nothing about car purchases, as OKIGBO had maintained, but instead referred to "Atlas Extension Fee."

61. Once again, OKIGBO withdrew the proceeds of the Bank A scam. For example, according to bank records I have reviewed, on or about December 15, 2016, OKIGBO wrote a check to herself in the amount of $2,400 with the memo "payment for parts."

62. According to bank records I have reviewed, and a bank employee I have interviewed, Bank D closed the Bank D Account on or about February 28, 2017 due to suspicious transactions with the account.

KNOWLEDGE OF CRIMINAL ORIGIN OF PROCEEDS

63. To prove the offense of money laundering, the government must show that a defendant knew the proceeds were from some form of unlawful activity, though not necessarily which type of unlawful activity—so long as the proceeds were in fact from a specified unlawful activity, in this case, wire fraud. The evidence outlined in this affidavit establishes probable cause that OKIGBO knew that the proceeds were from criminal activity.

64. There are a number of indicia discussed in this affidavit establishing probable cause that OKIGBO knew the proceeds were from unlawful activity, and was not mistaken as to their source:

a. First: OKIGBO lied to a Bank A investigator about knowing the victims who were wiring her money.

b. Second: OKIGBO continued to open accounts at new banks in the name of U4CS to receive payments from victims and purchase cars even after bank after bank closed her accounts, and multiple wires were flagged, frozen, or recalled.

c. Third: not a single incoming wire transfer mentioned payments for cars. Rather, whenever a memo accompanied an incoming wire, it referred to items such as "Payment for Administrative Charges and Court Documents," and "The Waiver Fee Payment of

Administrative Charge," which are at odds with the ostensible business OKIGBO said she was running.

d. Fourth: numerous victims from around the world were instructed by the perpetrators of the Bank A scam to wire money to OKIGBO's accounts over a two-year period, and virtually all of the deposits into those accounts during that period were proceeds of the Bank A scam.

e. Fifth: OKIGBO opened *Bank A* Account #1 the day before she received her *first* wire from a *Bank A* scam victim, a $100,000 wire transfer, at which time she already had an account at Bank B open in the name of U-4CS.

CONCLUSION

65. In total, from in or about November 2014 to in or about January 2017, across the six different bank accounts discussed in this affidavit, OKIGBO received and withdrew, transferred, or spent a total of over $4 million from victims of the Bank A scam.

66. Based on the forgoing, I submit there is probable cause that, from in or about November 2014 until present, in the Southern District of Texas and elsewhere, OKIGBO has knowingly and willfully conspired to commit money laundering, in violation of 18 U.S.C. § 1956(h), and, on such basis, request that a complaint charging her with such offense, along with a warrant for her arrest, be issued.

REQUEST FOR SEALING

67. I further request that the Court order that all papers in support of this complaint, including the affidavit and arrest warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation.

Respectfully submitted,

Special Agent John Chiue, FBI

Subscribed and sworn to before me on November, 14 2017, and I find probable cause

Honorable Frances H. Stacy
UNITED STATES MAGISTRATE JUDGE